LISTING OF CLAIMS:

Claim 1 (currently amended) A remotely accessible secure cryptographic system for storing a plurality of private cryptographic keys to be associated with a ~~plurality of~~ multiple users, wherein ~~the~~ said cryptographic system associates each of ~~the plurality of~~ said multiple users with one or more different keys from ~~the~~ said plurality of private cryptographic keys and performs cryptographic functions for each user using the associated one or more different keys without releasing ~~the~~ said plurality of private cryptographic keys to ~~the~~ said users, the cryptographic system comprising:

a depository system having at least one server which stores a plurality of private cryptographic keys and a plurality of enrollment authentication data, wherein each enrollment authentication data identifies one of multiple users and each of ~~the~~ said multiple users is associated with one or more different keys from ~~the~~ said plurality of private cryptographic keys;

an authentication engine which compares authentication data received by one of ~~the~~ said multiple users to enrollment authentication data corresponding to ~~the~~ said one of multiple users and received from ~~the~~ said depository system, thereby producing an authentication result;

a cryptographic engine which, when ~~the~~ said authentication result indicates proper identification of ~~the~~ said one of the multiple users, performs cryptographic functions on behalf of the one of ~~the~~ said multiple users using the associated one or more different keys received from ~~the~~ said depository system; and

a transaction engine connected to route data from the multiple users to ~~the~~ said depository server system, ~~the~~ said authentication engine, and ~~the~~ said cryptographic engine.

Claim 2 (currently amended) A remotely accessible secure cryptographic system, comprising:

a depository system having at least one server which stores at least one private key and a plurality of enrollment authentication data, wherein each enrollment authentication data identifies one of multiple users;

an authentication engine which compares authentication data received by one of ~~the~~ said multiple users to enrollment authentication data corresponding to ~~the~~ said one of multiple users and received from ~~the~~ said depository system, thereby producing an authentication result;

a cryptographic engine which, when ~~the~~ said authentication result indicates proper identification of ~~the~~ said one of ~~the~~ said multiple users, performs cryptographic functions on behalf of ~~the~~ said one of ~~the~~ said multiple users using at least said private key received from ~~the~~ said depository system; and

a transaction engine connected to route data from ~~the~~ said multiple users to ~~the~~ said depository server system, ~~the~~ said authentication engine, and ~~the~~ said cryptographic engine.

Claim 3 (currently amended) The cryptographic system of Claim 2, wherein ~~the~~ said depository system further comprises a plurality of data storage facilities, each data storage facility having at least one server storing a substantially randomized portion of ~~the~~ said private key and a substantially randomized portion of ~~the~~ said plurality of enrollment authentication data.

Claim 4 (original) The cryptographic system of Claim 3, wherein each substantially randomized portion is individually undecipherable.

Claim 5 (currently amended) The cryptographic system of Claim 2, wherein ~~the~~ said enrollment authentication data includes biometric data.

Claim 6 (currently amended) The cryptographic system of Claim 5, wherein ~~the~~ said biometric data includes finger print patterns.

Claim 7 (currently amended) The cryptographic system of Claim 2, wherein ~~the~~ said at least one private key corresponds to ~~the~~ said secure cryptographic system.

Claim 8 (currently amended) The cryptographic system of Claim 2, wherein ~~the~~ said at least one private key corresponds to ~~the~~ said one of ~~the~~ said multiple users.

Claim 9 (currently amended) The ~~trust engine~~ cryptographic system of Claim 2, wherein ~~the~~ said cryptographic functions comprise one of digital signing, encryption, and decryption.

Claim 10 (currently amended) A method of facilitating cryptographic functions, ~~the~~ said method comprising:

associating a user from multiple users with one or more keys from a plurality of private cryptographic keys stored on a secure server;

receiving authentication data from ~~the~~ said user;

comparing ~~the~~ said authentication data to authentication data corresponding to ~~the~~ said user, thereby verifying the identity of ~~the~~ said user; and

utilizing ~~the~~ said one or more keys to perform cryptographic functions without releasing ~~the~~ said one or more keys to ~~the~~ said user.

Claim 11 (currently amended) The method of Claim 10, wherein ~~the~~ said authentication data corresponding to ~~the~~ said user was acquired prior to the step of receiving authentication data from ~~the~~ said user.

Claim 12 (original) The method of Claim 10, further comprising receiving a hash of a message or document.

Claim 13 (currently amended) The method of Claim 12, further comprising archiving ~~the~~ said hash.

Claim 14 (currently amended) An authentication system for uniquely identifying a user through secure storage of ~~the~~ said user's enrollment authentication data, ~~the~~ said authentication system comprising:

a plurality of data storage facilities, wherein each data storage facility includes a computer accessible storage medium which stores one of portions of enrollment authentication data; and

an authentication engine which communicates with ~~the~~ said plurality of data storage facilities and comprises

a data splitting module which operates on ~~the~~ said enrollment authentication data to create portions,

a data assembling module which processes the portions from at least two of ~~the~~ said data storage facilities to assemble ~~the~~ said enrollment authentication data, and

a data comparator module which receives current authentication data from a user and compares the current authentication data with the assembled enrollment authentication data to determine whether ~~the~~ said user has been uniquely identified.

Claim 15 (currently amended) The authentication system of Claim 14, wherein ~~the~~ said portions are not individually decipherable.

Claim 16 (currently amended) The authentication system of Claim 14, wherein ~~the~~ said each data storage facility is logically separated from any other data storage facility.

Claim 17 (currently amended) The authentication system of Claim 14, wherein ~~the~~ said each data storage facility is physically separated from any other data storage facility.

Claim 18 (currently amended) The authentication system of Claim 14, further comprising a cryptographic engine which, upon the unique identification of ~~the~~ said user by ~~the~~ said authentication engine, provides cryptographic functionality to ~~the~~ said user.

Claim 19 (currently amended) The authentication system of Claim 14, wherein ~~the~~ said plurality of data storage facilities comprises at least one secure server.

Claim 20 (currently amended) The authentication system of Claim 14, wherein unique identification of ~~the~~ said user by ~~the~~ said authentication engine provides ~~the~~ said user authorization to gain access to or to operate one or more systems.

Claim 21 (currently amended) The authentication system of Claim 20, wherein ~~the~~ said one or more systems include one or more electronic devices.

Claim 22 (currently amended) The authentication system of Claim 20, wherein ~~the~~ said one or more systems include one or more computer software systems.

Claim 23 (currently amended) The authentication system of Claim 20, wherein ~~the~~ said one or more systems include one or more consumer electronics.

Claim 24 (currently amended) The authentication system of Claim 23, wherein ~~the~~ said one or more consumer electronics includes a cellular phone.

Claim 25 (currently amended) The authentication system of Claim 20, wherein ~~the~~ said one or more systems include one or more cryptographic systems.

Claim 26 (currently amended) The authentication system of Claim 20, wherein ~~the~~ said one or more systems include one or more physical locations.

Claim 27 (currently amended) The authentication system of Claim 14, wherein at least one of ~~the~~ said data storage facilities stores at least some of sensitive data, wherein ~~the~~ said at least one of ~~the~~ said data storage facilities serves ~~the~~ said sensitive data when ~~the~~ said authentication engine indicates that ~~the~~ said user has been uniquely identified.

Claim 28 (currently amended) The authentication system of Claim 14, further comprising a data vault which stores sensitive data, wherein ~~the~~ said data vault serves ~~the~~ said sensitive data when ~~the~~ said authentication engine indicates that ~~the~~ said user has been uniquely identified.

Claim 29 (currently amended) The authentication system of Claim 14, wherein ~~the~~ said authentication system engine outputs an indication of whether ~~the~~ said user has been uniquely identified.

Claim 30 (currently amended) A cryptographic system, comprising:

a plurality of data storage facilities, wherein each data storage facility includes a computer accessible storage medium which stores one of portions of cryptographic keys; and

a cryptographic engine which communicates with ~~the~~ said plurality of data storage facilities and comprises

a data splitting module which operate on ~~the~~ said cryptographic keys to create portions,

a data assembling module which processes the portions from at least two of ~~the~~ said data storage facilities to assemble ~~the~~ said cryptographic keys, and

a cryptographic handling module which receives ~~the~~ said assembled cryptographic keys and performs cryptographic functions therewith.

Claim 31 (currently amended) The cryptographic system of Claim 30, wherein ~~the~~ said portions are not individually decipherable.

Claim 32 (currently amended) The cryptographic system of Claim 30, wherein ~~the~~ said each data storage facility is logically separated from any other data storage facility.

Claim 33 (currently amended) The cryptographic system of Claim 30, wherein ~~the~~ said each data storage facility is physically separated from any other data storage facility.

Claim 34 (currently amended) The cryptographic system of Claim 30, further comprising an authentication engine which, before the cryptographic functionality may be employed on behalf of a user, uniquely identifies ~~the~~ said user.

Claim 35 (currently amended) The cryptographic system of Claim 30, wherein ~~the~~ said plurality of data storage facilities comprises at least one secure server.

Claim 36 (currently amended) A method of storing authentication data in geographically remote secure data storage facilities thereby protecting ~~the~~ said authentication data against comprise compromise of any individual data storage facility, ~~the~~ said method comprising:

receiving authentication data at a trust engine;

combining at ~~the~~ said trust engine ~~the~~ said authentication data with a first substantially random value to form a first combined value;

combining ~~the~~ said authentication data with a second substantially random value to form a second combined value;

creating a first pairing of ~~the~~ said first substantially random value with ~~the~~ said second combined value;

creating a second pairing of ~~the~~ said first substantially random value with ~~the~~ said second substantially random value;

storing ~~the~~ said first pairing in a first secure data storage facility; and

storing ~~the~~ said second pairing in a second secure data storage facility remote from ~~the~~ said first secure data storage facility.

Claim 37 (currently amended) A method of storing authentication data comprising:

receiving authentication data;

combining ~~the~~ said authentication data with a first set of bits to form a second set of bits;

combining ~~the~~ said authentication data with a third set of bits to form a fourth set of bits;

creating a first pairing of ~~the~~ said first set of bits with ~~the~~ said third set of bits;

creating a second pairing of ~~the~~ said first set of bits with ~~the~~ said fourth set of bits;

storing one of ~~the~~ said first and second pairings in a first computer accessible storage medium; and

storing the other of ~~the~~ said first and second pairings in a second computer accessible storage medium.

Claim 38 (currently amended) The method of Claim 37, wherein at least one of ~~the~~ said first and second computer accessible storage mediums comprises at least one server.

Claim 39 (currently amended) The method of Claim 37, wherein ~~the~~ said first computer accessible storage medium is geographically remote from ~~the~~ said second computer accessible storage medium.

Claim 40 (currently amended) The method of Claim 37, wherein the matching of one of ~~the~~ said first and second pairings with one of ~~the~~ said first and second computer accessible storage mediums is substantially random.

Claim 41 (currently amended) The method of Claim 37, wherein at least one of ~~the~~ said first and third sets of bits are substantially random.

Claim 42 (currently amended) The method of Claim 37, wherein at least one of ~~the~~ said first and third sets of bits comprises a bit length equal to a bit length of ~~the~~ said sensitive data.

Claim 43 (currently amended) The method of Claim 37, wherein both ~~the~~ said first and second pairings are needed to reassemble ~~the~~ said data.

Claim 44 (currently amended) The method of Claim 37, further comprising:

creating a third pairing of ~~the~~ said second set of bits with ~~the~~ said third set of bits;

creating a fourth pairing of ~~the~~ said second set of bits with ~~the~~ said fourth set of bits;

storing one of ~~the~~ said third and fourth pairings in a third computer accessible storage medium; and

storing the other of ~~the~~ said third and fourth pairings in a fourth computer accessible storage medium.

Claim 45 (currently amended) A method of storing cryptographic data in geographically remote secure data storage facilities thereby protecting ~~the~~ said cryptographic data against compromise of any individual data storage facility, ~~the~~ said method comprising:

receiving cryptographic data at a trust engine;

combining at ~~the~~ said trust engine ~~the~~ said cryptographic data with a first substantially random value to form a first combined value;

combining ~~the~~ said cryptographic data with a second substantially random value to form a second combined value;

creating a first pairing of ~~the~~ said first substantially random value with ~~the~~ said second combined value;

creating a second pairing of ~~the~~ said first substantially random value with ~~the~~ said second substantially random value;

storing ~~the~~ said first pairing in a first secure data storage facility; and

storing ~~the~~ said second pairing in a secure second data storage facility remote from ~~the~~ said first secure data storage facility.

Claim 46 (currently amended) A method of storing cryptographic data comprising:

receiving authentication data;

combining ~~the~~ said cryptographic data with a first set of bits to form a second set of bits;

combining ~~the~~ said cryptographic data with a third set of bits to form a fourth set of bits;

creating a first pairing of ~~the~~ said first set of bits with ~~the~~ said third set of bits;

creating a second pairing of ~~the~~ said first set of bits with ~~the~~ said fourth set of bits;

storing one of ~~the~~ said first and second pairings in a first computer accessible storage medium; and

storing the other of ~~the~~ said first and second pairings in a second computer accessible storage medium.

Claim 47 (currently amended) The method of Claim 46, wherein at least one of ~~the~~ said first and second computer accessible storage mediums comprises at least one server.

Claim 48 (currently amended) The method of Claim 46, wherein ~~the~~ said first computer accessible storage medium is geographically remote from ~~the~~ said second computer accessible storage medium.

Claim 49 (currently amended) The method of Claim 46, wherein the matching of one of ~~the~~ said first and second pairings with one of ~~the~~ said first and second computer accessible storage mediums is substantially random.

Claim 50 (currently amended) The method of Claim 46, wherein at least one of ~~the~~ said first and third sets of bits are substantially random.

Claim 51 (currently amended) The method of Claim 46, wherein at least one of ~~the~~ said first and third sets of bits comprises a bit length equal to a bit length of ~~the~~ said sensitive data.

Claim 52 (currently amended) The method of Claim 46, wherein both ~~the~~ said first and second pairings are needed to reassemble ~~the~~ said cryptographic data.

Claim 53 (currently amended) The method of Claim 46, further comprising:

creating a third pairing of ~~the~~ said second set of bits with ~~the~~ said third set of bits;

creating a fourth pairing of ~~the~~ said second set of bits with ~~the~~ said fourth set of bits;

storing one of ~~the~~ said third and fourth pairings in a third computer accessible storage medium; and

storing the other of ~~the~~ said third and fourth pairings in a fourth computer accessible storage medium.

Claim 54 (currently amended) A method of handling sensitive data in a cryptographic system, wherein ~~the~~ said sensitive data exists in a useable form only during actions employing ~~the~~ said sensitive data, ~~the~~ said method comprising:

receiving in a software module, substantially randomized sensitive data from a first computer accessible storage medium;

receiving in ~~the~~ said software module, substantially randomized data from a second computer accessible storage medium,

processing ~~the~~ said substantially randomized sensitive data and ~~the~~ said substantially randomized data in ~~the~~ said software module to assemble ~~the~~ said sensitive data; and

employing ~~the~~ said sensitive data in a software engine to ~~perform an action, wherein~~ ~~the~~ said ~~action includes one of authenticating~~ authenticate a user ~~and performing a cryptographic function~~.

Claim 55 (currently amended) The method of Claim 54, further comprising destroying ~~the~~ said sensitive data after completion of ~~the~~ said action.

Claim 56 (currently amended) The method of Claim 54, wherein ~~the~~ said sensitive data includes one of user biometric data and cryptographic key data.

Claim 57 (currently amended) The method of Claim 54, wherein at least one of ~~the~~ said first and second computer accessible storage mediums comprise a secure server.

Claim 58 (currently amended) The method of Claim 54, wherein ~~the~~ said software module comprises a data assembling module and ~~the~~ said software engine comprises one of an authentication engine and a cryptographic engine.

Claim 59 (currently amended) A secure authentication system, comprising:

a plurality of authentication engines, wherein each authentication engine receives enrollment authentication data designed to uniquely identify a user to a degree of certainty, each authentication engine receives current authentication data to compare to ~~the~~ said enrollment authentication data, and wherein each authentication engine determines an authentication result; and

a redundancy system which receives ~~the~~ said authentication result of at least two of ~~the~~ said authentication engines and determines whether ~~the~~ said user has been uniquely identified.

Claim 60 (currently amended) The secure authentication system of Claim 59, wherein ~~the~~ said redundancy system determines whether ~~the~~ said user has been uniquely identified by following the majority of ~~the~~ said authentication results.

Claim 61 (currently amended) The secure authentication system of Claim 59, wherein ~~the~~ said redundancy system determines whether ~~the~~ said user has been uniquely identified by requiring ~~the~~ said authentication results to be unanimously positive before issuing a positive identification.

Claim 62 (currently amended) The secure authentication system of Claim 59, wherein ~~the~~ said redundancy system includes a plurality of redundancy modules, and ~~the~~ said secure authentication system further comprises:

a plurality of geographically remote trust engines, each trust engine having one of ~~the~~ said plurality of authentication engines and one of ~~the~~ said redundancy modules,

wherein the redundancy module for at least one of ~~the~~ said plurality of trust engines determines whether ~~the~~ said user has been uniquely identified using ~~the~~ said authentication results from ones of ~~the~~ said authentication engines associated with the other trust engines and without using ~~the~~ said authentication results from the at least one trust engine.

Claim 63 (currently amended) The secure authentication system of Claim 62, wherein each of ~~the~~ said plurality of trust engines includes a depository having a computer accessible storage medium which stores a substantially randomized portion of ~~the~~ said enrollment authentication data and wherein each depository forwards ~~the~~ said substantially randomized portion of ~~the~~ said enrollment authentication data to ~~the~~ said plurality of authentication engines.

Claim 64 (currently amended) The secure authentication system of Claim 62, wherein ~~the~~ said determination of whether ~~the~~ said user has been uniquely identified corresponds to the one of ~~the~~ said redundancy modules to first determine a result.

Claim 65 (currently amended) A trust engine system for facilitating authentication of a user, ~~the~~ said trust engine system comprising:

a first trust engine comprising a first depository, wherein ~~the~~ said first depository includes a computer accessible storage medium which stores portions of enrollment authentication data;

a second trust engine located at a different geographic location than ~~the~~ said first trust engine and comprising:

a second depository having a computer accessible storage medium which stores portions of enrollment authentication data~~,~~;

an authentication engine communicating with ~~the~~ said first and second depositories and which assembles at least two portions of enrollment authentication data into a usable form~~,~~; and

a transaction engine communicating with ~~the~~ said first and second depositories and ~~the~~ said authentication engine,

wherein when ~~the~~ said second trust engine is determined to be available to execute a transaction, ~~the~~ said transaction engine receives authentication data from a user and forwards a request for the portions of enrollment authentication data to ~~the~~ said first and second

depositories, and wherein ~~the~~ said authentication engine receives ~~the~~ said authentication data from ~~the~~ said transaction engine and the portions of ~~the~~ said enrollment authentication data from ~~the~~ said first and second depositories, and determines an authentication result.

Claim 66 (currently amended) The trust engine system of Claim 65, wherein ~~the~~ said determination of whether ~~the~~ said second trust engine is available to execute ~~the~~ said transaction includes a determination of whether ~~the~~ said second trust engine is within geographic proximity to ~~the~~ said user.

Claim 67 (currently amended) The trust engine system of Claim 65, wherein ~~the~~ said determination of whether ~~the~~ said second trust engine is available to execute ~~the~~ said transaction includes a determination of whether ~~the~~ said second trust engine is currently servicing a light system load.

Claim 68 (currently amended) The trust engine system of Claim 65, wherein ~~the~~ said determination of whether ~~the~~ said second trust engine is available to execute ~~the~~ said transaction includes a determination of whether ~~the~~ said second trust engine is currently scheduled for maintenance.

Claim 69 (currently amended) The trust engine system of Claim 65, wherein ~~the~~ said first and second trust engines are determined to be available, and an authentication result for ~~the~~ said trust engine system follows ~~the~~ said first of ~~the~~ said first and second trust engines to produce ~~the~~ said authentication result.

Claim 70 (new) A method of handling sensitive data in a cryptographic system, wherein said sensitive data exists in a useable form only during actions employing said sensitive data, said method comprising:

receiving in a software module, substantially randomized sensitive data from a first computer accessible storage medium;

receiving in said software module, substantially randomized data from a second computer accessible storage medium,

processing said substantially randomized sensitive data and said substantially randomized data in said software module to assemble said sensitive data; and

employing said sensitive data in a software engine to perform a cryptographic function.

Claim 71 (new) The method of Claim 70, further comprising destroying said sensitive data after completion of said action.

Claim 72 (new) The method of Claim 70, wherein said sensitive data includes one of user biometric data and cryptographic key data.

Claim 73 (new) The method of Claim 70, wherein at least one of said first and second computer accessible storage mediums comprise a secure server.

Claim 74 (new) The method of Claim 70, wherein said software module comprises a data assembling module and said software engine comprises one of an authentication engine and a cryptographic engine.